PENTESTING

La ciberseguridad cada día va cobrando más importancia y con ello surgen nuevos métodos para reforzar las defensas de los sistemas operativos y el software empresarial. Así que si quieres evitar los ciberataques en tu pequeña, mediana o gran empresa, y conocer las vulnerabilidades de tu sistema para poder optimizarlo, **es importante que conozcas el *Pentesting*.**

Índice de Contenidos

- 1_¿Qué es Pentesting?
- 2_¿Cuáles son los tipos de Pentesting?
  - 2.1_Pentesting de caja negra
  - 2.2_Pentesting de caja blanca
  - 2.3_Pentesting de caja gris
- 3_¿Qué fases tiene el Pentesting?
  - 3.1_Recopilación y planificación
  - 3.2_Análisis de vulnerabilidades
  - 3.3_Modelado de amenazas
  - 3.4_Explotación del sistema
  - 3.5_Elaboración de los informes
  - 3.6_¿Conoces todas las consecuencias de los ciberataques?
- 4_Diferencias entre Pentesting y Análisis de Vulnerabilidades
- 5_¿Qué herramientas se usan en el Pentesting?
- 6_¿Cómo convertirse en Pentester?

¿Qué es *Pentesting*?

El *Pentesting* es un test de penetración que **valora los posibles fallos de seguridad informática** que puede tener un sistema y qué alcance tienen dichos fallos. Es el resultado de unir dos conceptos: ***penetration*** y ***testing***.

El proceso consiste en **simular un ataque cibernético** a la organización que se somete al test para intentar romper y sobrepasar sus sistemas de seguridad.

Los resultados obtenidos se trasladan a un informe que será entregado a la empresa para que con ello puedan **implementar mejoras** y **reforzar su ciberseguridad**.

Es un sistema muy eficaz para **evaluar el nivel de eficiencia que tienen las defensas** de la empresa y aumentar su seguridad.

¿Cuáles son los tipos de *Pentesting*?

Dependiendo de la cantidad de información sobre los sistemas informáticos que se van a testar, podemos clasificar el *Pentesting* en **tres tipos**:

Pentesting de caja negra

También conocido como *Black Box Pentesting*, en esta prueba **el testeador realiza sus análisis completamente a ciegas**, es decir, sin contar con información de ningún tipo sobre el sistema a evaluar. Por tanto el ataque lo realizará como si lo hiciera alguien totalmente ajeno a la empresa.

Al igual que se realizan simulacros de ataques aéreos, con un *Pentesting* de caja negra es posible simular un ciberataque a tu sistema informático, ya sea de un hacker o un ciberdelincuente.



Pentesting de caja blanca

También conocido como *White Box Pentesting*, en este tipo de prueba el testeador conoce todos los datos del sistema a evaluar (las contraseñas, firewalls o IPs del sistema informático, entre otros). Por tanto, **el ataque se simula como si fuese realizado por alguien de dentro**, es decir, alguien que forma parte de la empresa.

Es la prueba más completa de *Pentesting* al que puede someterse un sistema informático y con el que es posible **detectar con gran precisión** los aspectos mejorables de sus defensas.

Pentesting de caja gris

También conocido como *Grey Box Pentesting*, esta prueba **es un intermedio o mezcla de las dos anteriores**. En este caso el testeador contará con algo de información a la hora de realizar el test, aunque sigue siendo un buen simulacro de ataque ajeno al sistema.



¿Qué fases tiene el *Pentesting*?

Las **cinco fases** del *Pentesting* son:

- **Recopilación** y **planificación**.
- Análisis de **vulnerabilidades**.
- Modelado de **amenazas**.
- **Explotación** del sistema.
- Elaboración de los **informes**.

Recopilación y planificación

En esta primera fase **se definen los objetivos** del *Pentesting*, se determina qué sistemas se van a abordar y qué métodos se emplearán para hacerlo.

Además, es en esta fase cuando **el auditor recolecta todos los datos necesarios** para el test de penetración. Dependiendo del caso es posible que esta fase requiera de:

- Realizar **escaneos de IP**, dominios o puertos.
- Obtener **metadatos**.
- Hacer un **Google Hacking** (o dorking).
- Emplear **herramientas de scrapeo** y obtención de información como Nmap o SubFinder.

Análisis de vulnerabilidades

En esta segunda fase **se analiza cómo responde el sistema a una intrusión** y buscar los puntos más débiles. Esta fase, junto a la anterior, son las necesarias para poder definir definitivamente el alcance que tendrá el *pentest*.

Modelado de amenazas

Una vez se tiene clara la estrategia a seguir, se procede a explotar las vulnerabilidades detectadas para modelar las posibles amenazas frente a las que el sistema debería poder defenderse y **definir qué mejoras son necesarias**.

Explotación del sistema

Esta es la fase en la que **se simulan los ataques al sistema**, con el objetivo de evaluar las amenazas, cómo el sistema responde ante ellas e informar al propietario sobre la verdadera vulnerabilidad de su sistema.

Además, en algunos casos, en esta fase se intenta **llevar al límite las defensas del sistema** para afinar aún más los resultados del *pentest*.

Elaboración de los informes

En esta fase es donde se cumple el objetivo final del *Pentesting*, que no es otro que **informar a la empresa de los resultados** de un ataque simulado para que pueda implementar mejoras y reforzar sus sistemas de seguridad.

Lo más habitual es emitir dos informes. Por un lado un **informe técnico** para los administradores del sistema informático y por otro un **informe ejecutivo** para los directivos de la empresa.

¿Conoces todas las consecuencias de los ciberataques?

Diferencias entre *Pentesting* y Análisis de Vulnerabilidades

Como hemos visto en las fases del *Pentesting*, **el análisis de vulnerabilidades es solo una parte del mismo**.

En un análisis de vulnerabilidades el objetivo es detectar los puntos débiles del sistema, mientras que en el *Pentesting* lo que se hace es **atacar esos puntos para valorar su actuación** y poder determinar las mejoras a implementar.

¿Qué herramientas se usan en el *Pentesting*?

Para cada fase del *Pentesting* existen herramientas informáticas que pueden ser de utilidad. Algunos ejemplos son; usar herramientas como **Nmap**, **Dnsrecon** o **SubFinder** para escanear sistemas e incluso detectar sus puntos débiles.

BurpSuite y Nessus son las *pentesting tools* más habituales y **detectan puntos débiles en sistemas o webs** mediante un análisis en profundidad y contrastación con amplias bases de datos.

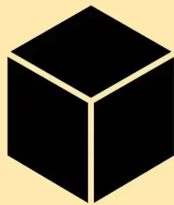
Otras herramientas como **Metasploit** miden el alcance de las vulnerabilidades, una vez detectadas; **John the Ripper** sirve para descifrar contraseñas e incluso hay herramientas como Veil que sirven para enmascarar código malicioso.

Por último, comentar que existe la posibilidad de realizar *Pentesting* con **Python**, lo que facilita el proceso por ser un lenguaje informático muy flexible, multipropósito, potente y fácil de aprender.




¿Qué es el **Pentesting**?

El *Pentesting* es una **prueba de ciberseguridad**, que consiste en simular un ataque cibernético a tu propio sistema, para comprobar su nivel de defensa.



Pentesting **de caja negra**

El ataque se realiza **completamente a ciegas**, sin conocer ningún dato sobre el sistema que se pone a prueba. Es la mejor forma de simular un ciberataque real.

Pentesting **de caja blanca**

En este tipo de ataque, **se conocen todos los datos sobre el sistema** (contraseñas, IP's, etc) por lo que se busca simular cómo sería un ciberataque desde dentro de la organización o empresa.





Pentesting **de caja gris**

El pentesting de caja gris es una **mezcla de los otros dos tipos**: se conocen solo algunos datos del sistema antes de hacer la prueba.

Fuente: https://nuclio.school/que-es-el-pentesting/